UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,436	02/28/2002	Zhichen Xu	10018744-1	6233

7590 04/10/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 04/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/084,436	XU ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on January 13, 2006. All Independent **claims 1, 14, 18, 22 and 24** have been amended and dependent claim 9 is also amended. No claim has been canceled. Therefore claims **1-36** are pending and are examined.

Response to Arguments

2. Applicant's arguments with respect to the claims **1-2,8-19,24-25,31-36** have been considered but are moot in view of the new ground(s) of rejection.

3. Applicant's arguments with respect to the c**laims 3-7,20-23 and 26-30** have been fully considered but they are not persuasive.

Applicant in particular points out the rejection made to claim 22.

Applicant argued that some of the limitation in independent claim 22 is not disclosed by the combination of the references namely Walker and Herz.

Examiner disagrees with the argument.

Examiner asserts the fact that each and every limitation of the claims is disclosed by the combination of the references.

In order to make clear how each and every limitation of claim 22 is disclosed by the combination of the references on the record, Examiner would point out the following.

Walker discloses an apparatus for increasing privacy in a computer network including peers operable to exchange information via the network,wherein the peers include computing platforms, the apparatus comprising:

at least one processor; [figure 2, ref. Num "205" and figure 4, "405"]

memory coupled to said at least one processor; [figure 2, 215 & 220]

and a privacy module residing in said memory and said privacy module executed by said at least one processor, wherein said privacy module is configured to receive a message at said data provider [figure 2, 210], said message comprises:

> A mix configured to provide a path among a plurality of the peers between a data provider and a data requestor in the network, wherein the mix includes an anonymous identity of each of the plurality of peers in the path [Column 35,lines 14-18;column 36, lines 40-41; Column 35, lines 14-18 and column 35, lines 19-30; column 36, lines 40-41] ;
>
> **an encrypted reference to requested data encrypted with a first encryption key [column 35, lines 63-column 36, line 6]**(the first encryption key is a key generated by carol K_3/the 3rd trusted peer/computer and the reference N shown on column 36, lines 1, which is included in the message from Alice is encrypted as shown on column 36, lines 6 (X_4)]**; an encrypted first encryption key protected with a public key of said data requester;** [Column 35, lines 36-column 36, line 10] (encrypted first encryption key generated by carol which is K_3 is also protected or encrypted with the public key of Bob) **and said privacy module is also configured to decrypt said first encryption key with a complementary encryption key to said public key of said data provider [column 36, lines 11-13]** (Bob receives M_1 and decrypt the first encryption key K_3 with a complementary/private key of BOB) and decrypts said data reference with said encryption key and once he gets the decrypted first encryption key K_3, he decrypts the X_4, included in

the message to verify the signature. Therefore the N which meets the limitation of end user request identifier is decrypted.)

Walker does not explicitly disclose a mix configured to provide a path

However, in the field of endeavor Herz discloses

A mix configured to provide a path wherein the mix includes an anonymous identity of each of the plurality of peers in the path.[column 39, lines 3-17; lines18-23 and column 39, line 66-column 40, line 6; column 37, lines 50-52; column 39, lines 3-7]

Furthermore Herz discloses,

The user's client processor C3 forms a signed message **S(R, SK.sub.P),** which is paired with the user's pseudonym P and (if the request R requires airesponse) a secure one-time set of return envelopes, to form a message M. It protects the message M with a multiply enveloped route for the outgoing path. The enveloped route s provide for secure communication **between S1 and the proxy server S2**. The message M is enveloped in the most deeply nested message and is therefore difficult to recover should the message be intercepted by an eavesdropper. 2. The message M is sent by client C3 to its local server S1, and is then routed by the data communication network. **N from server S1 through a set of mixes as dictated by the outgoing envelope set and arrives** at the **selected proxy server S2.** 3. The proxy server **S2 separates the received message M into the request message R, the pseudonym P, and (if included) the set of envelopes for the return path. The proxy server S2 uses pseudonym P to index and retrieve the corresponding record in proxy server S2's database**, which record is stored in local storage at the proxy server S2 or on other distributed storage media accessible to. proxy server S2 via the

network N. This, record contains a public key PK.sub.P, user-specific information, and credentials associated with pseudonym P. The proxy server S2 uses the public key PK.sub.P to check that the signed version S(R, SK.sub.P) of request message R is valid. [column 39, lines 8-35]

For the motivation refer to the rejection below. Therefore each and every limitation of claim 22 is disclosed by the references on the record.

As to the argument raised by the applicant referring to the dependent claims which depend on claim 22, examiner points out that these claims stands and fall with the independent claim 22.

The rejection remains valid unless and otherwise the claims are further amended and overcome the ground of rejection without introducing new matter.

Claim Objections

4. Claim 4 is objected to because of the following informalities: Dependent claim 4 depends on itself.

For the purpose of examination, it is assumed that claim 4 depends on claim 3.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-36** are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (hereinafter referred as Walker) (U.S. Patent No 5,862,223) in view of Herz (hereinafter referred as Herz) ((U.S. Patent No 6,460,036) (filed on Dec 5, 1997)

7. **As per claim 1, 8,12,15,17-18, 24, 31-32 Walker discloses** a method of increasing peer privacy in a computer network including peers operable to exchange information via network, wherein the peers include computing platforms, [column 35, lines 14-17] the method comprising:

Receiving a request for data from a data requester,[column 35, 45-47; column 35, lines 15-17] (Bob's computer receives Alice request through the 3rd trusted party central controller/carol's computer as described on column 35, lines 33-34)

Determining whether a data provider exits that stores the requested data wherein the data provider is a peer of the peers;[Abstract, figure 2, ref: Num "270";column 8, 22-27 and column 35, lines 29-67] (As explained on abstract, the present invention includes a controller having a database for storing expert qualifications. In one embodiment, the controller receives an expert request/requested data. A search program identifies experts qualified to respond to the expert request/requested data. The expert request/requested data is then transmitted **to the expert/data provider,** which results in **an expert answer transmitted** to and received by the central controller. As explained on column 8, lines 22-27, once the Exchange contains enough experts in a given subject, each new application may be reviewed by other experts who are already members of the Exchange. **This provides a basis for peer review** that can be used to maintain assurance of qualifications. As explained on column 35, line

32b, Bob's computer is also qualified expert. Bob's computer is acts as both client and server when interacts with carol's computer and is assumed to be a modern PC which meets the limitation of a peer and since there are a number of experts, the qualified expert who would be selected to provide the an expert answer, or Bob's computer meets the limitation of peer of peers and carol's computer or the central controller determines whether a data provider for instance Bob's computer exists that stores the requested data)

Selecting a plurality of peers to form a path between said data provider and said data requestor,[Abstract, column 35, lines 14-17;column 36, lines 40-42; column 8, lines 52-53, experts/data providers/peers can be chosen or selected as disclosed on column 8, lines 52-53; therefore if the experts answers comes from a plurality of experts for the same data request, the controller will inherently form a path between said provider and data requestor] **wherein said data provider and said data requester are the respective ends of said path**;[column 36, lines 40-42, column 35, lines 45-column 36, lines 42] **generating a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path;[Column 35, lines 14-18 and column 35, lines 19-30; column 36, lines 40-41] and transmitting said mix to said data provider** [column 36, lines 9-10 and figure 29]. (carol's computer sends M_1 to Bob/data provider via anonymous mix 180 meets the limitation of transmitting said mix to said data provider.)

Walker does not explicitly disclose generating a mix according to said path

However, in the field of endeavor Herz discloses

Generating a mix according to said path wherein the mix includes an anonymous identity of each of the plurality of peers in the path.[column 39,

lines 3-17; lines18-23 and column 39, line 66-column 40, line 6; column 37, lines 50-52; column 39, lines 3-7]

Furthermore, Herz discloses determining whether a data provider exits that stores the requested data wherein the data provider is a peer of the peers;[column 38, lines 39-42; figure 2, ref. Num "S4"; column 38, lines 31-47]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of generating a mix according to the path wherein the mix includes an anonymous identity of each of the plurality of peers in the path as per teachings of Herz in to the method as taught by **Walker,** in order to provide a secure communication and protection against eavesdropper.[See Herz, column 39, lines 8-line 17 and column 40, lines 3-6]

8. **As per claims 2,16,19 and 25 the combination of Walker and Herz discloses** a method as applied to claim above. Furthermore Walker discloses the method further comprising: generating a first encryption key; and encrypting said first encryption key with a public encryption key of said data provider. [**[column 35, lines 63-column 36, line 6]**(The first encryption key is a key k_3 is generated by carol/the 3rd trusted peer/computer and the first encryption key generated by carol which is K_3 is also protected or encrypted with the public key of Bob as shown on column 36, lines 3, x_3, and line 11)

9. **As per claims 9-11,13-14, 33-36 Walker discloses a method of increasing peer privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms,** [column 36, lines 40-41; column 35, lines 14-28 and column 35, line 29-column 36, line 41] **the method comprising:**

receiving a message comprising a mix at a current peer, wherein the mix includes an anonymous identity of each of a plurality of peers in a path between a data provider and a data requestor in the network[column 36, lines 40-41, column 35, lines 63, carol receives message comprising mix from Alice]; **modifying said mix by applying a complementary encryption key of said current peer to said mix**;[column 36, lines 7, M_1 which modifies said mix by applying encryption key] **retrieving a subsequent peer to said current peer; modifying said message with said modified mix; and transmitting said modified message to said subsequent peer.**[column 36, lines 11, c, carlos after retrieving a subsequent peer/bob to said current peer/carol; it modifies said message with said modified mix and send it to subsequent peer bob as it is described on column 35, lines 63-column 36, lines 11 and figure 29]

Walker does not explicitly disclose generating a mix according to said path

However, in the field of endeavor Herz discloses

Generating a mix according to said path wherein the mix includes an anonymous identity of each of the plurality of peers in the path.[column 39, lines 3-17; lines18-23 and column 39, line 66-column 40, line 6; column 37, lines 50-52; column 39, lines 3-7]

Furthermore, Herz discloses determining whether a data provider exits that stores the requested data wherein the data provider is a peer of the peers;[column 38, lines 39-42; figure 2, ref. Num "S4"; column 38, lines 31-47]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of generating a mix according to the path wherein the mix includes an anonymous identity of each of the plurality of peers in the path as per teachings of Herz in to the method as taught

by **Walker,** in order to provide a secure communication and protection against eavesdropper.[See Herz, column 39, lines 8-line 17 and column 40, lines 3-6]

10. **As per claims 3-7, 20-23 and 26- 30 Walker discloses** an apparatus for increasing privacy in a computer network including peers operable to exchange information via the network,wherein the peers include computing platforms, the apparatus comprising:

at least one processor; [figure 2, ref. Num "205" and figure 4, "405"]

memory coupled to said at least one processor; [figure 2, 215 & 220]

and a privacy module residing in said memory and said privacy module executed by said at least one processor, wherein said privacy module is configured to receive a message at said data provider [figure 2, 210], said message comprises:

A mix configured to provide a path among a plurality of the peers between a data provider and a data requestor.in the network, wherein the mix includes an anonymous identity of each of the plurality of peers in the path [Column 35,lines 14-18;column 36, lines 40-41; Column 35, lines 14-18 and column 35, lines 19-30; column 36, lines 40-41] ;

an encrypted reference to requested data encrypted with a first encryption key [column 35, lines 63-column 36, line 6](the first encryption key is a key generated by carol K_3/the 3rd trusted peer/computer and the reference N shown on column 36, lines 1, which is included in the message from Alice is encrypted as shown on column 36, lines 6 (X_4)]**; an encrypted first encryption key protected with a public key of said data requester;** [Column 35, lines 36-column 36, line 10] (encrypted first encryption key generated by carol which is K_3 is also protected or encrypted with the public key of Bob) **and said privacy**

module is also configured to decrypt said first encryption key with a complementary encryption key to said public key of said data provider [column 36, lines 11-13] (Bob receives M_1 and decrypt the first encryption key K_3 with a complementary/private key of BOB) and decrypts said data reference with said encryption key and once he gets the decrypted first encryption key K_3, he decrypts the X_4, included in the message to verify the signature. Therefore the N which meets the limitation of end user request identifier is decrypted.)

Walker does not explicitly disclose a mix configured to provide a path

However, in the field of endeavor Herz discloses

A mix configured to provide a path wherein the mix includes an anonymous identity of each of the plurality of peers in the path.[column 39, lines 3-17; lines18-23 and column 39, line 66-column 40, line 6; column 37, lines 50-52; column 39, lines 3-7]

Furthermore Herz discloses,

The user's client processor C3 forms a signed message **S(R, SK.sub.P),** which is paired with the user's pseudonym P and (if the request R requires airesponse) a secure one-time set of return envelopes, to form a message M. It protects the message M with a multiply enveloped route for the outgoing path. The enveloped route s provide for secure communication **between S1 and the proxy server S2**. The message M is enveloped in the most deeply nested message and is therefore difficult to recover should the message be intercepted by an eavesdropper. 2. The message M is sent by client C3 to its local server S1, and is then routed by the data communication network. **N from server S1**

> **through a set of mixes as dictated by the outgoing envelope set and arrives** at the **selected proxy server S2.** 3. The proxy server **S2 separates the received message M into the request message R, the pseudonym P, and (if included) the set of envelopes for the return path. The proxy server S2 uses pseudonym P to index and retrieve the corresponding record in proxy server S2's database**, which record is stored in local storage at the proxy server S2 or on other distributed storage media accessible to. proxy server S2 via the network N. This, record contains a public key PK.sub.P, user-specific information, and credentials associated with pseudonym P. The proxy server S2 uses the public key PK.sub.P to check that the signed version S(R, SK.sub.P) of request message R is valid. [column 39, lines 8-35]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of **configuring a mix to provide a path** wherein the mix includes an anonymous identity of each of the plurality of peers in the path as per teachings of Herz in to the method as taught by **Walker,** in order to provide a secure communication and protection against eavesdropper.[See Herz, column 39, lines 8-line 17 and column 40, lines 3-6]

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L
March 26, 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100